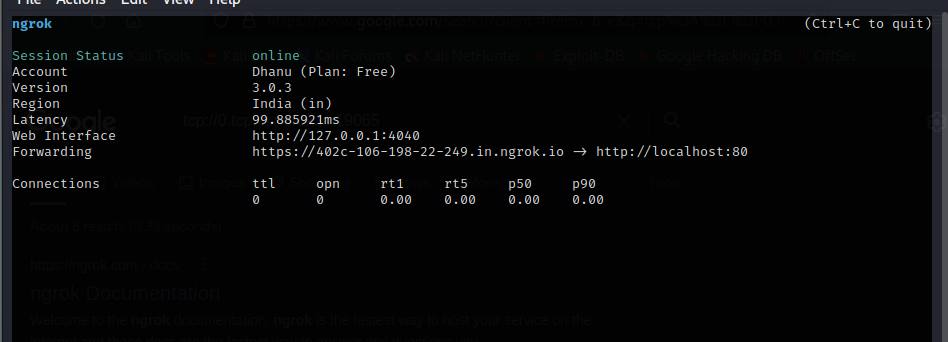
**1. Perform Social Engineering attack on the victim’s Android phone. Interpret**

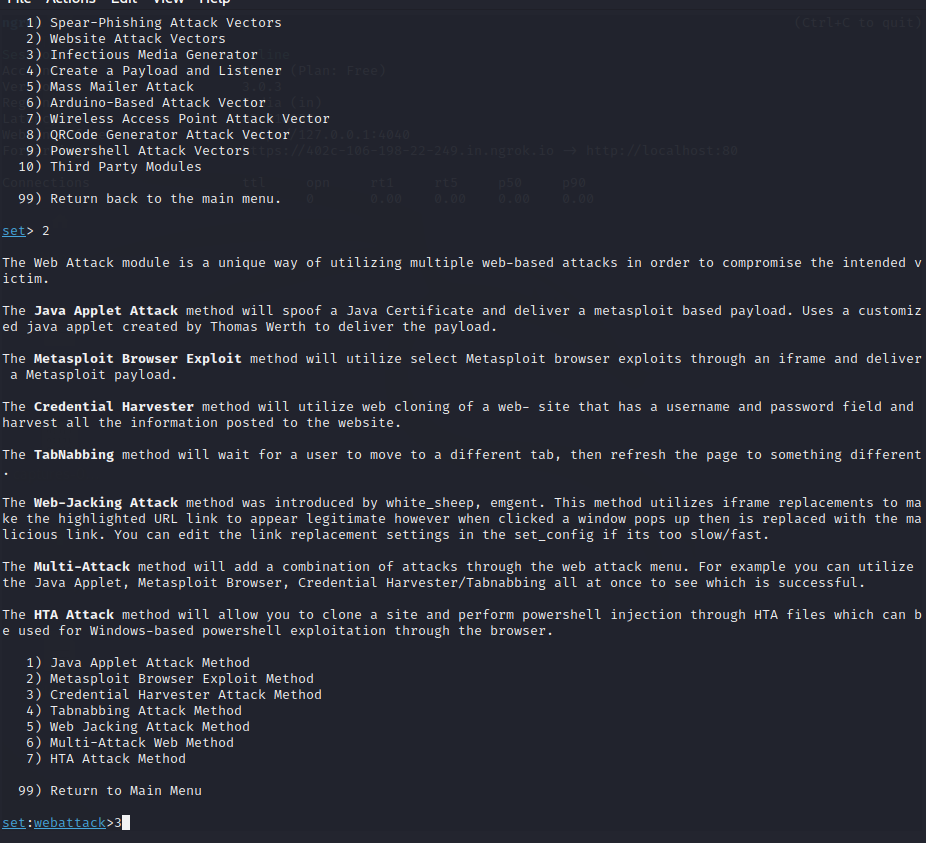
**your results.**

* Turn on the http tunnel in ngrok.



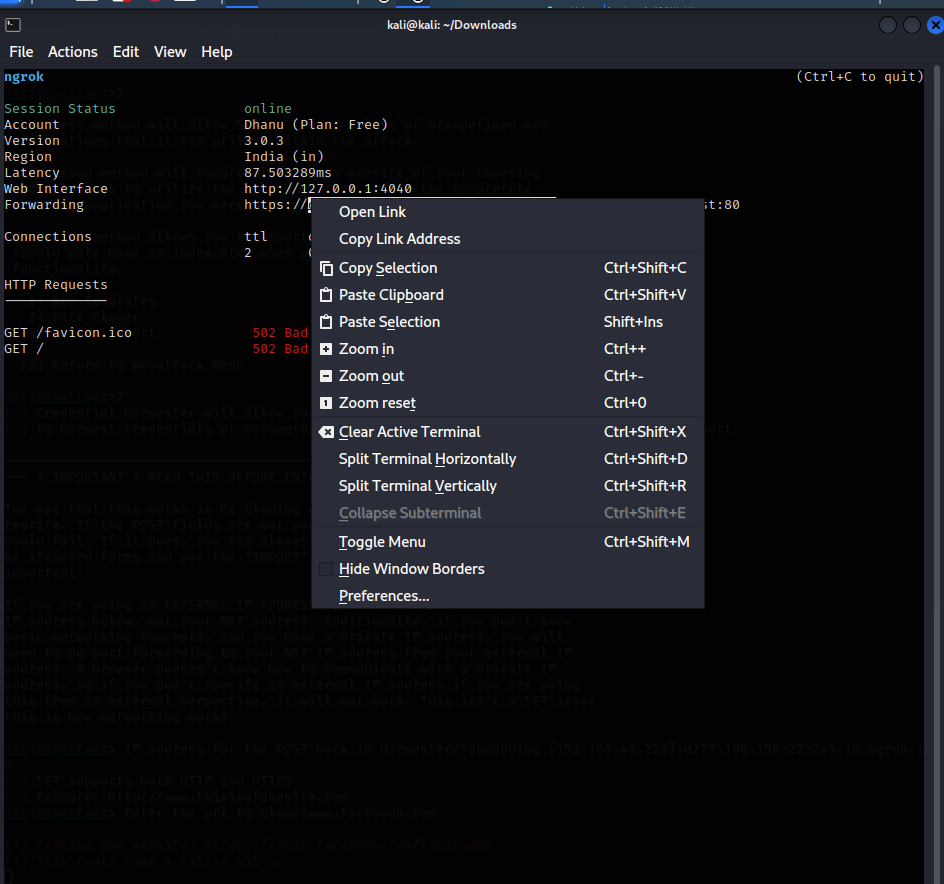


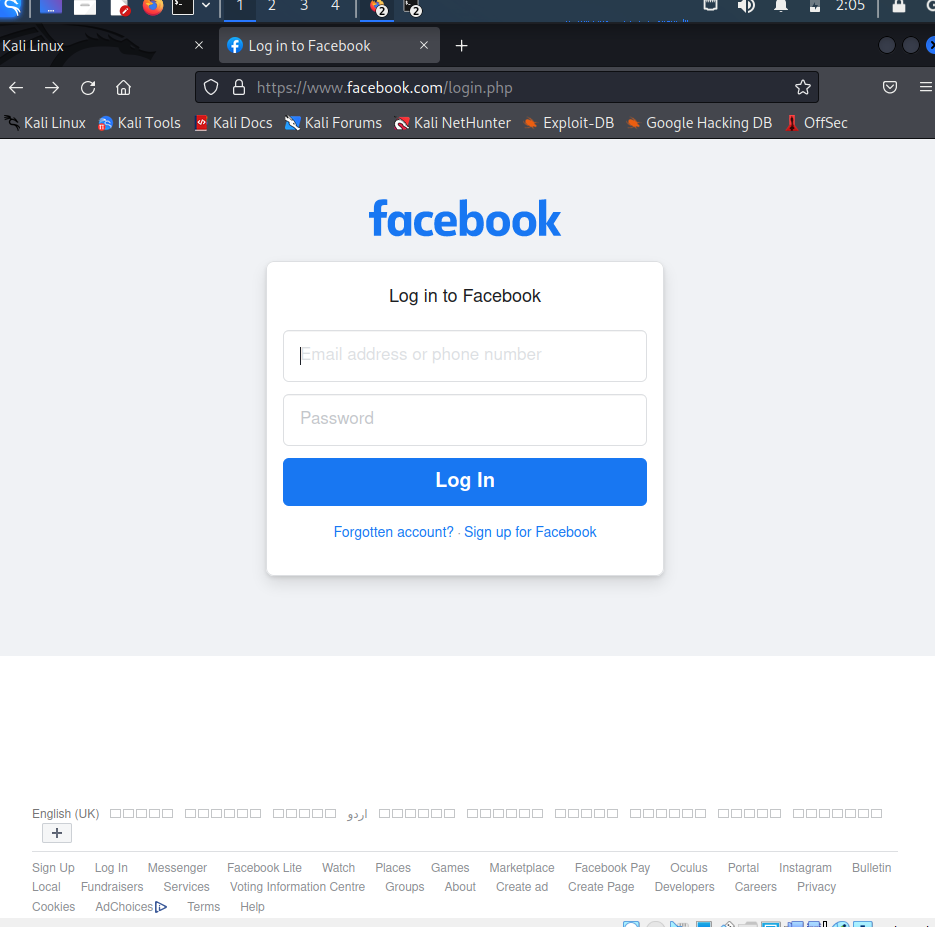
Setoolkit

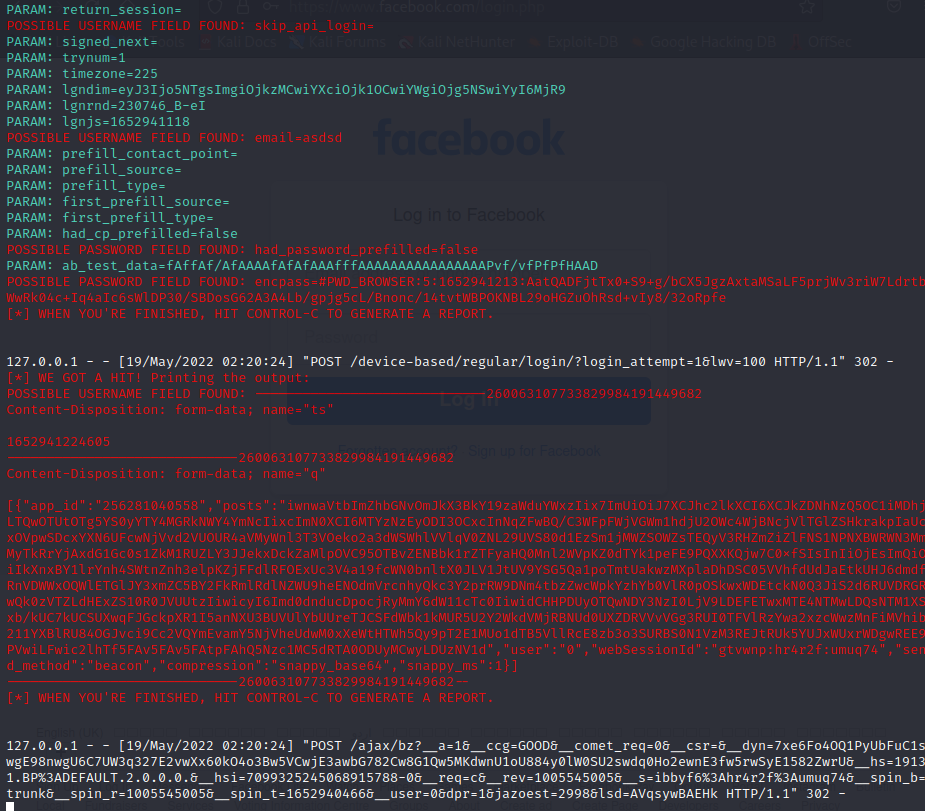




Open the forwardin link

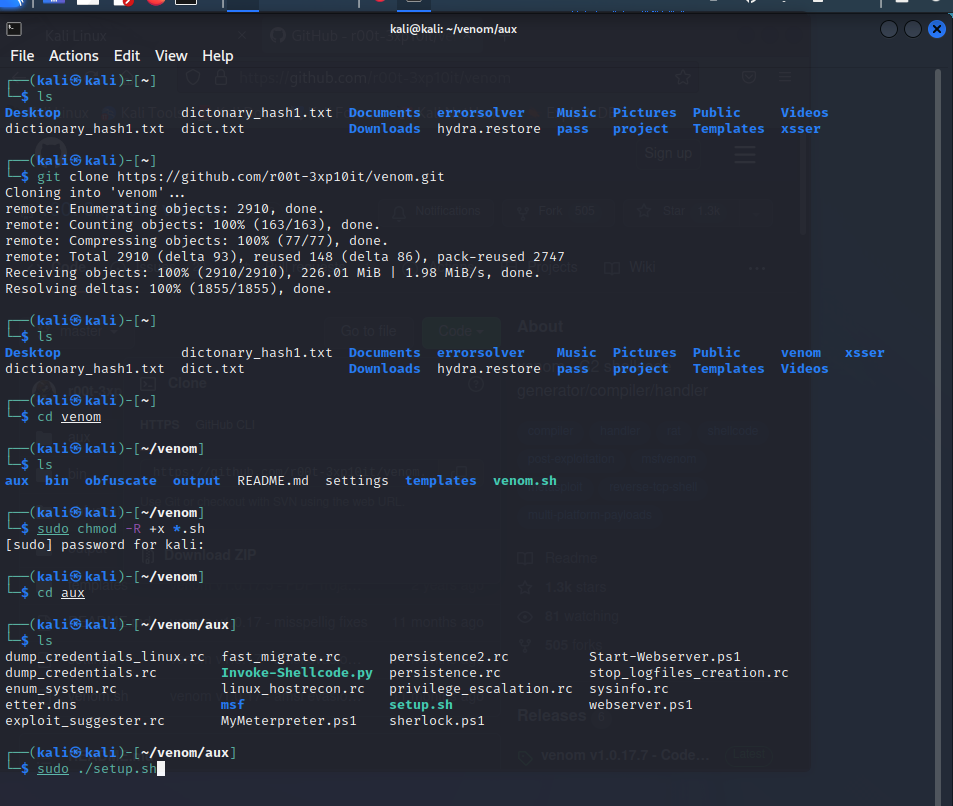


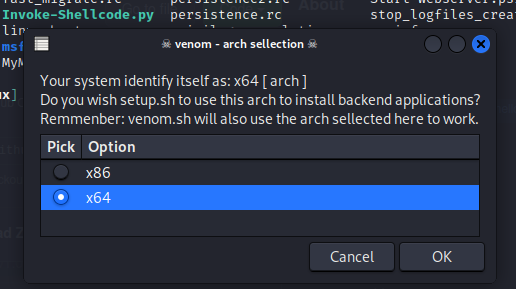


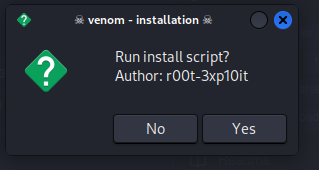


**Generate an .apk file to hack the password and the videos watched by the victim using**

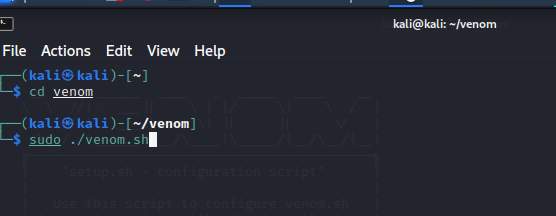
**his/her android mobile.**

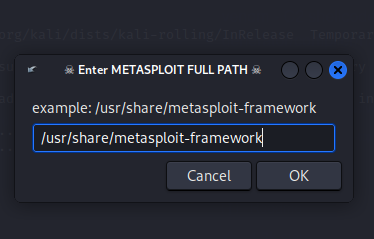


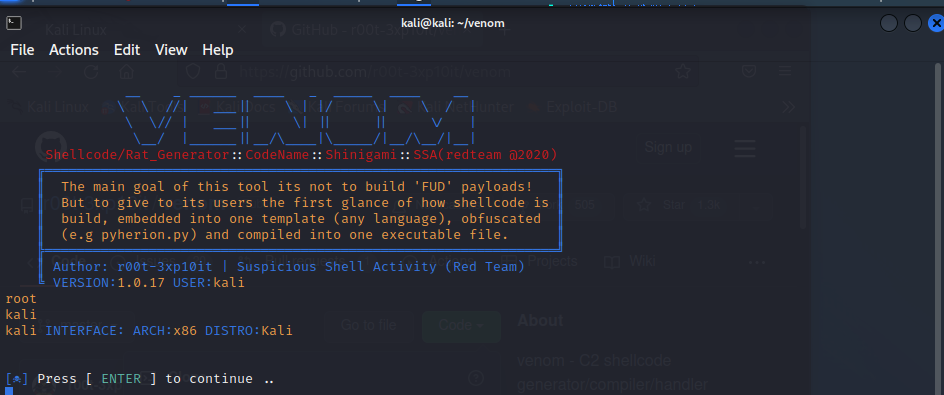


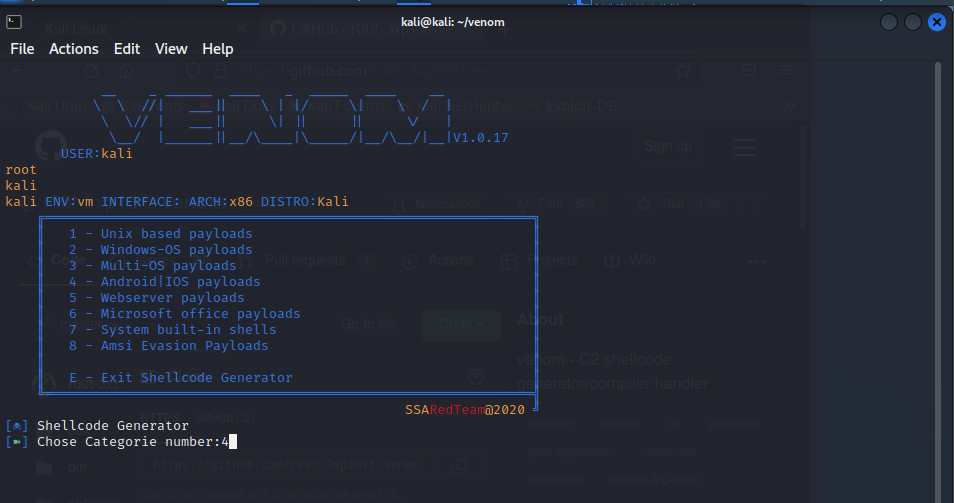


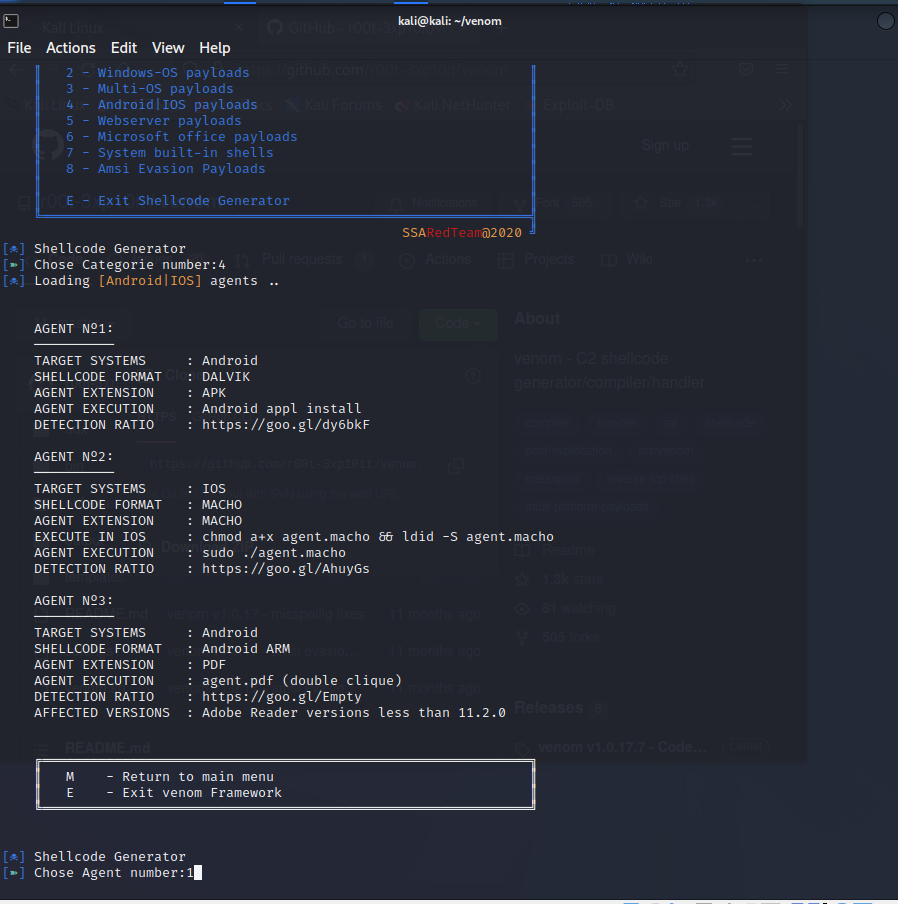
Venom shell installation

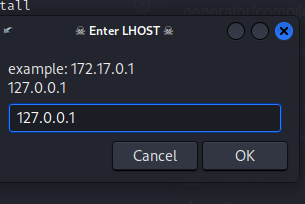


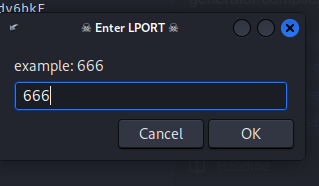


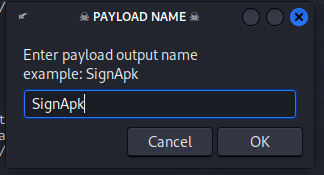


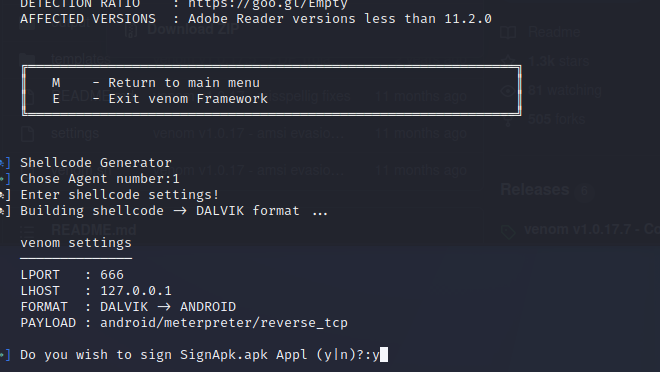




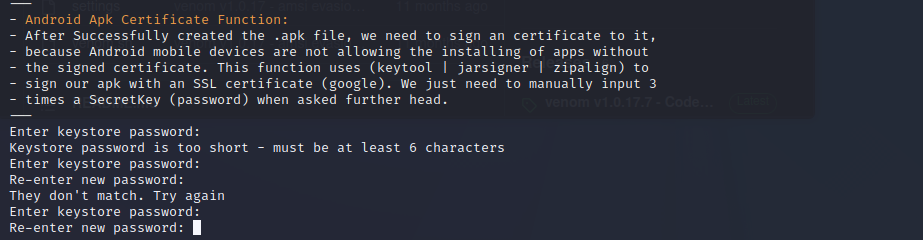


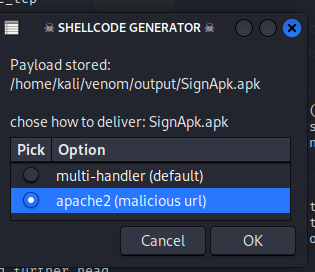


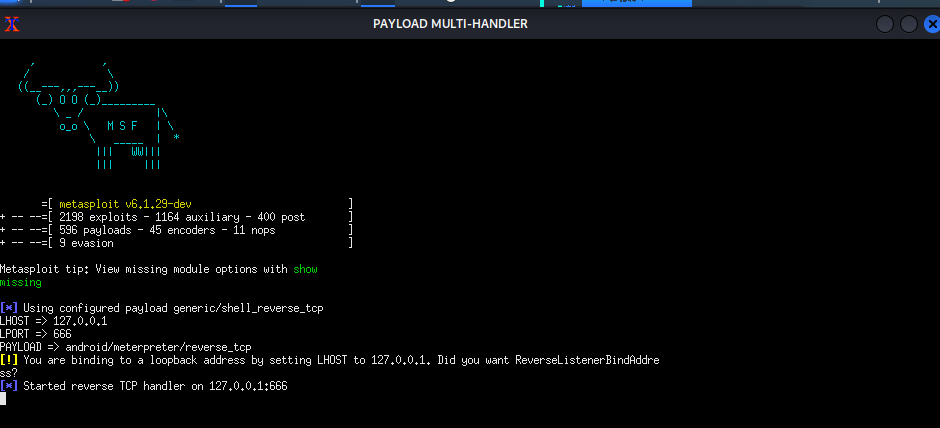


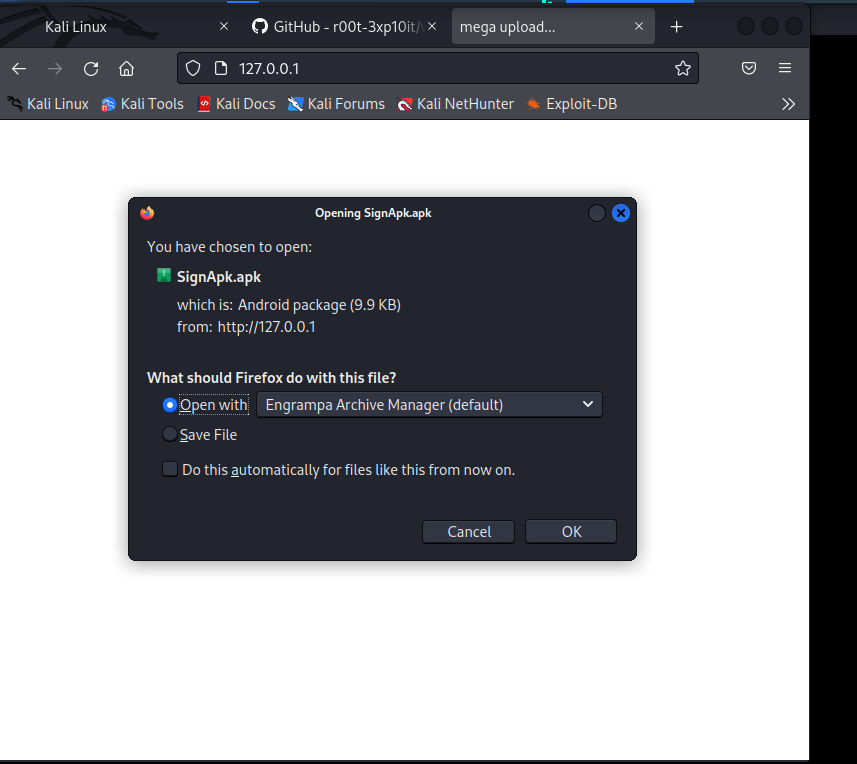


abcd@1234









This apk file is sent to the victim to retrieve their datas.

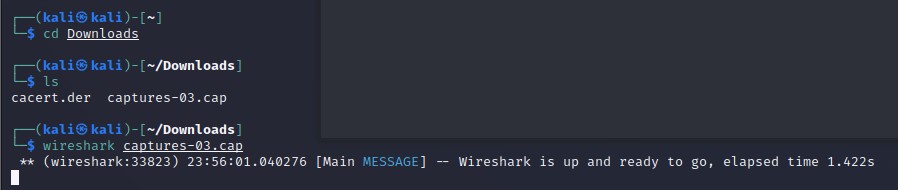
**2. Perform hidden SSID detection.**

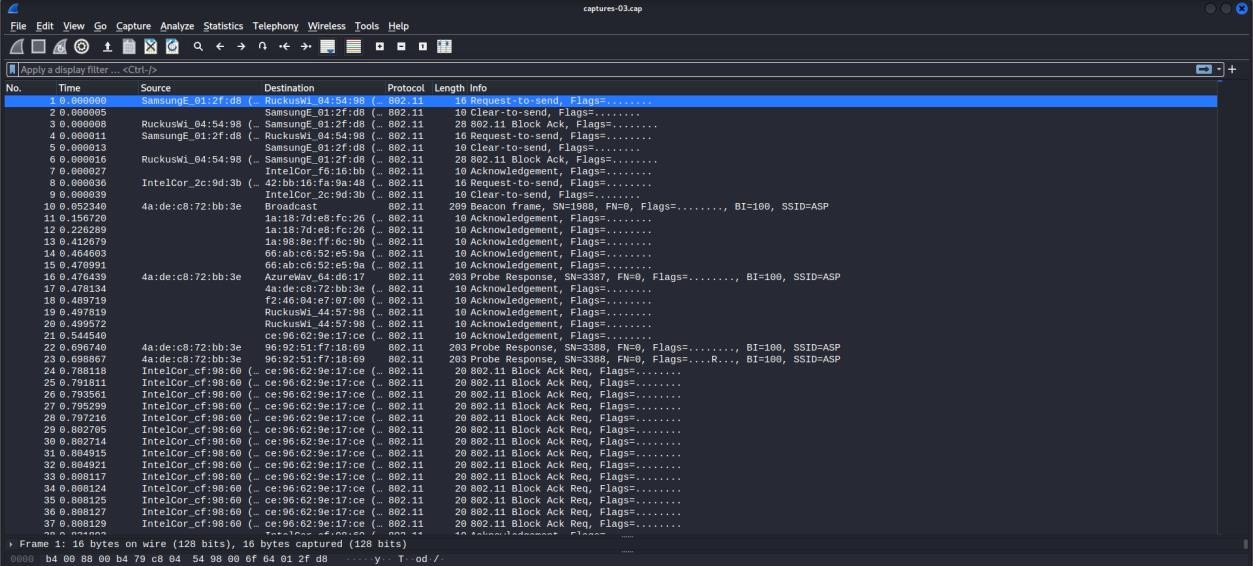
**Detect the SSID using airodump-ng, mdk3 and Wireshark using wireless**

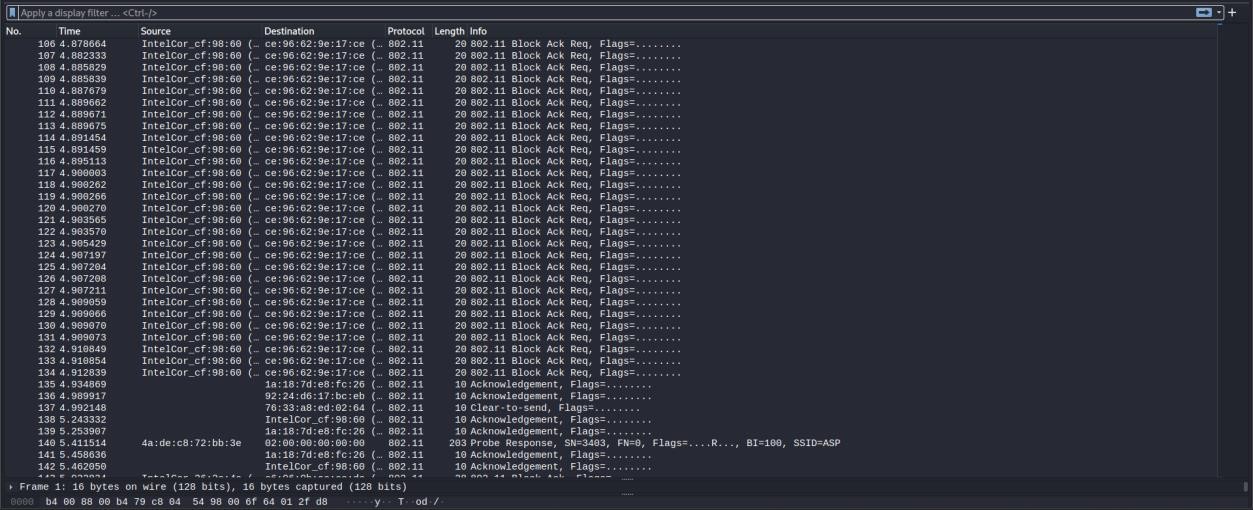
**penetration testing. Justify the process.**

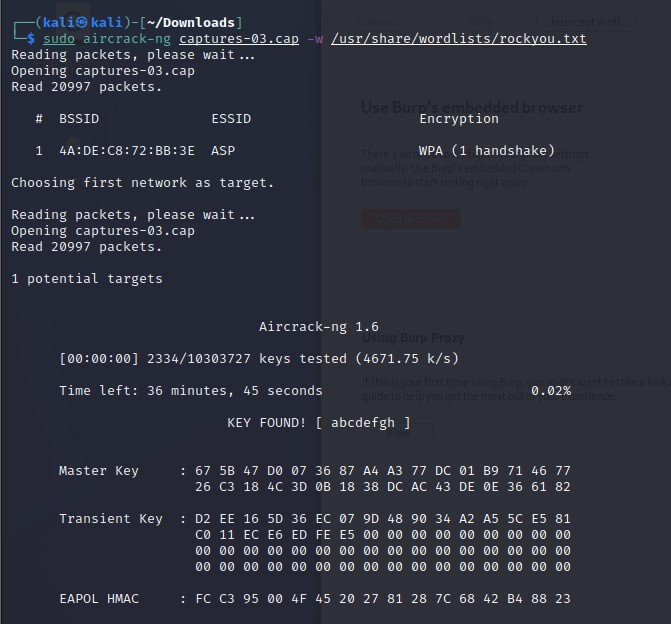
Text

Description automatically generated



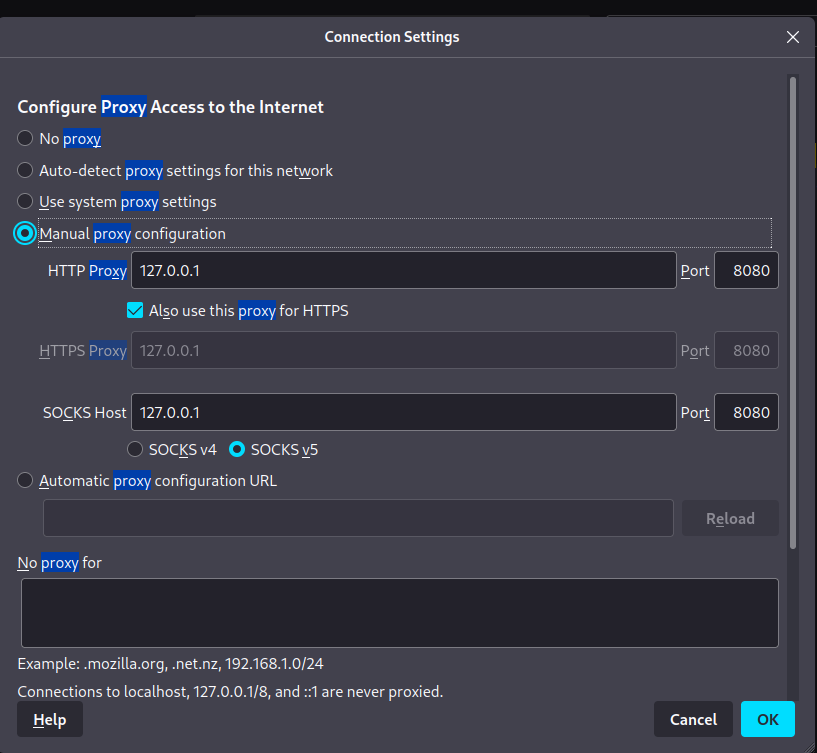






**3. Perform bruteforce attack on the website http://testphp.vulnweb.com/ using burpsuit.**

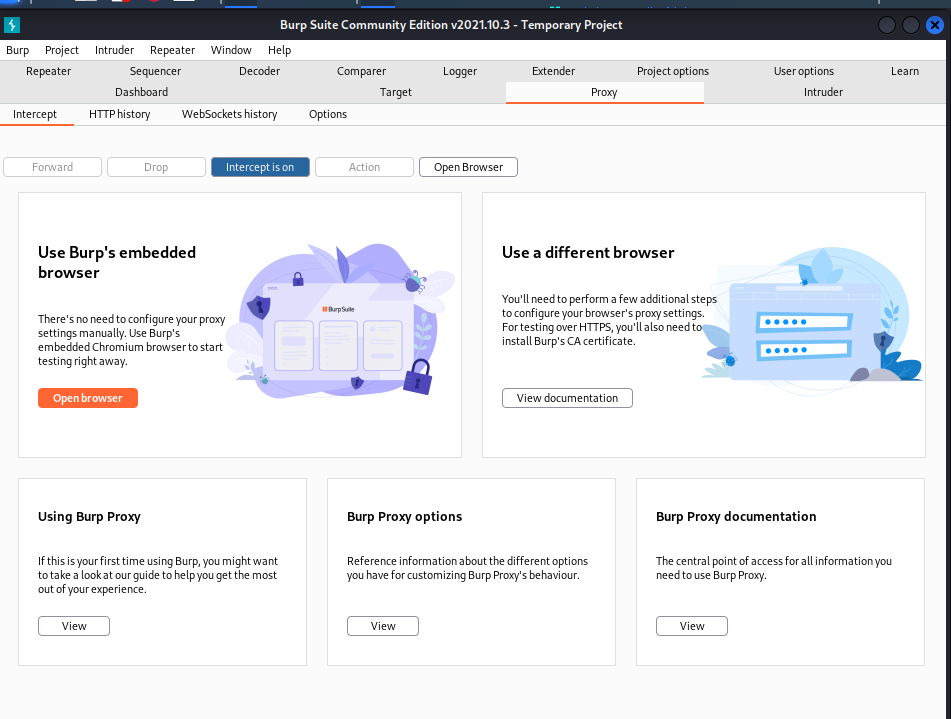
* In firefox->settings-> proxy->manual -> 127.0.0.1



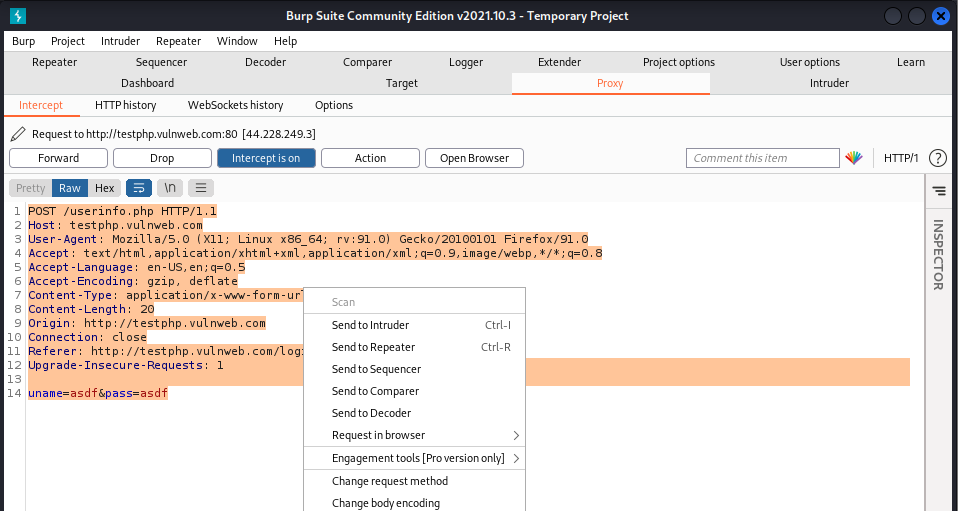
* Open <http://testphp.vulnweb.com/> in firefox -> enter to signup type some username and password.



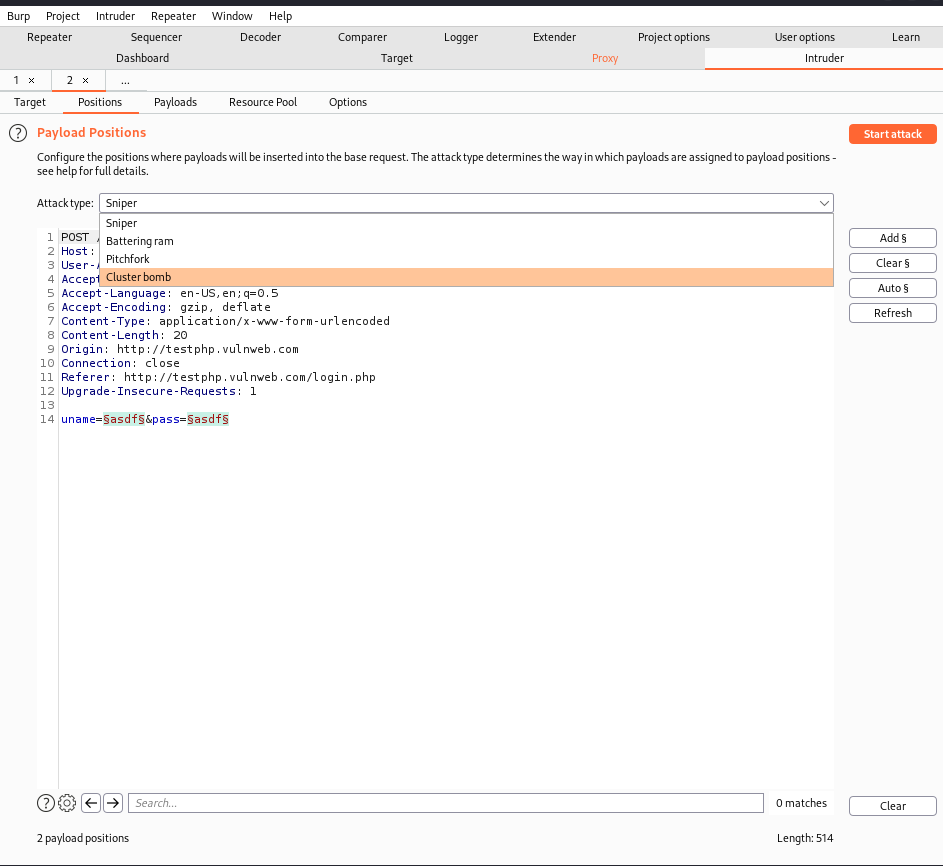
* Before pressing login open burpsuit from applications->intercept->turn on.



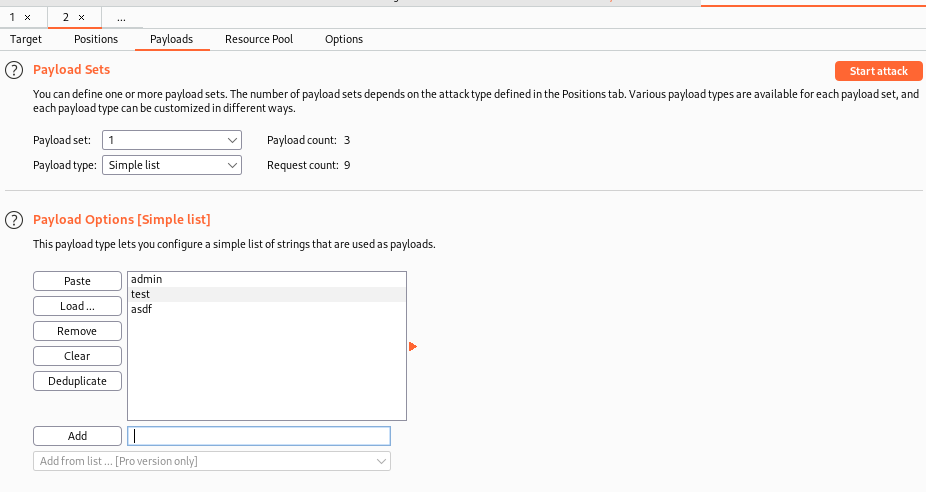
* Then now press the ligin button-> then navigate to burpsuit -> select the raw -> right click -> sent to intruder.



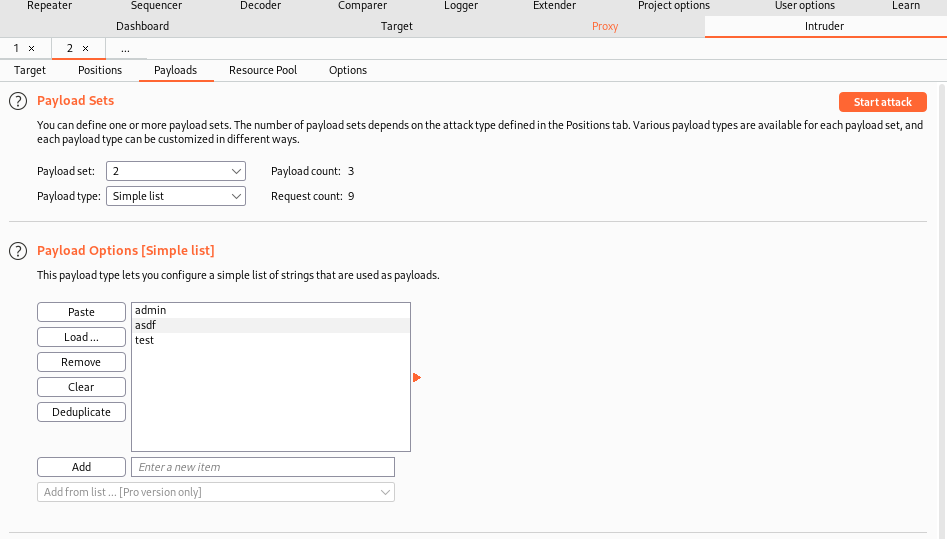
* Then in intruder -> select the positions tab-> choose the attack type as cluster bomb.



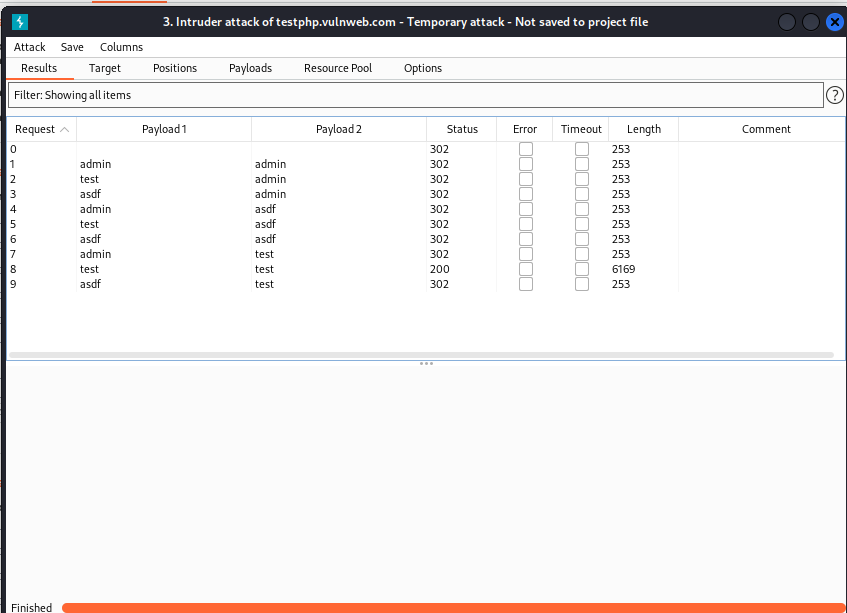
* Move to payloads tab enter the brute force passwords. Again select 2 enter those passwords by add.



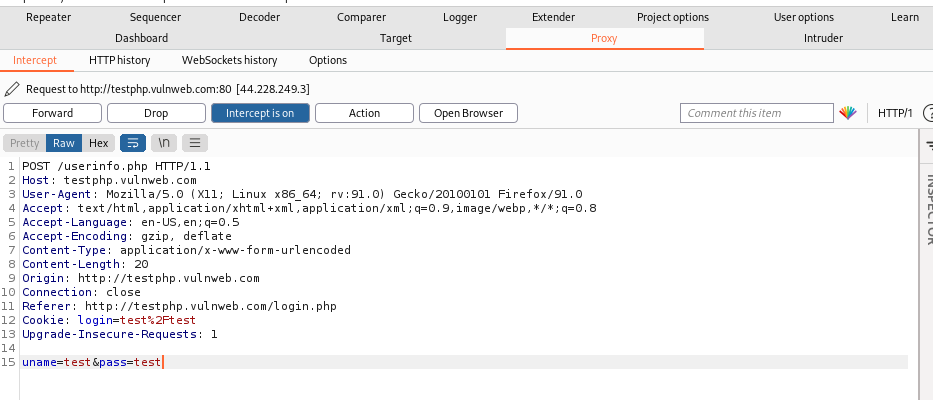


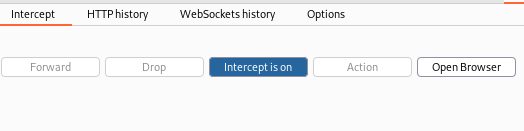


* Then click start to attack -> where the payload attack happens incase of actual password we would be able view status as 200 here it is test.

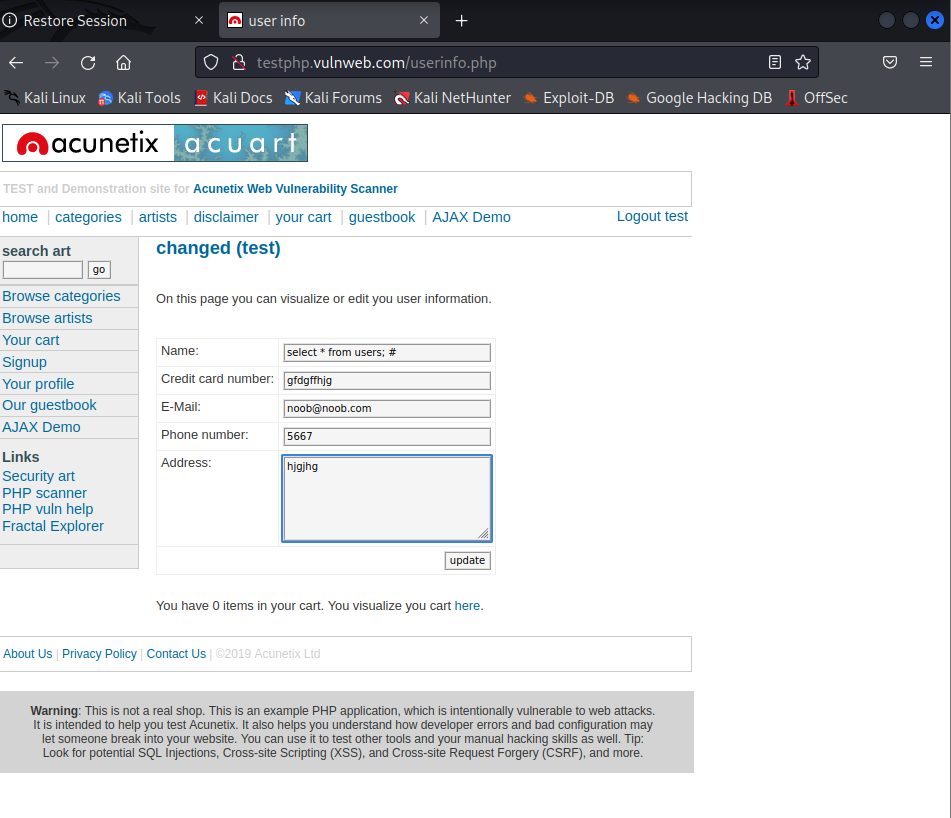


* Now move to intercept change the uname and passwd as test then click forward.

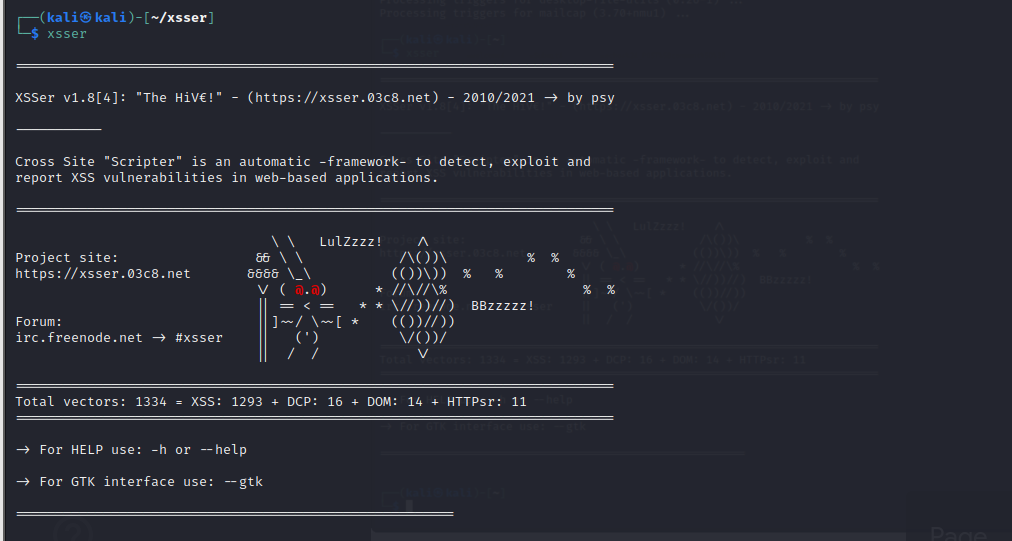


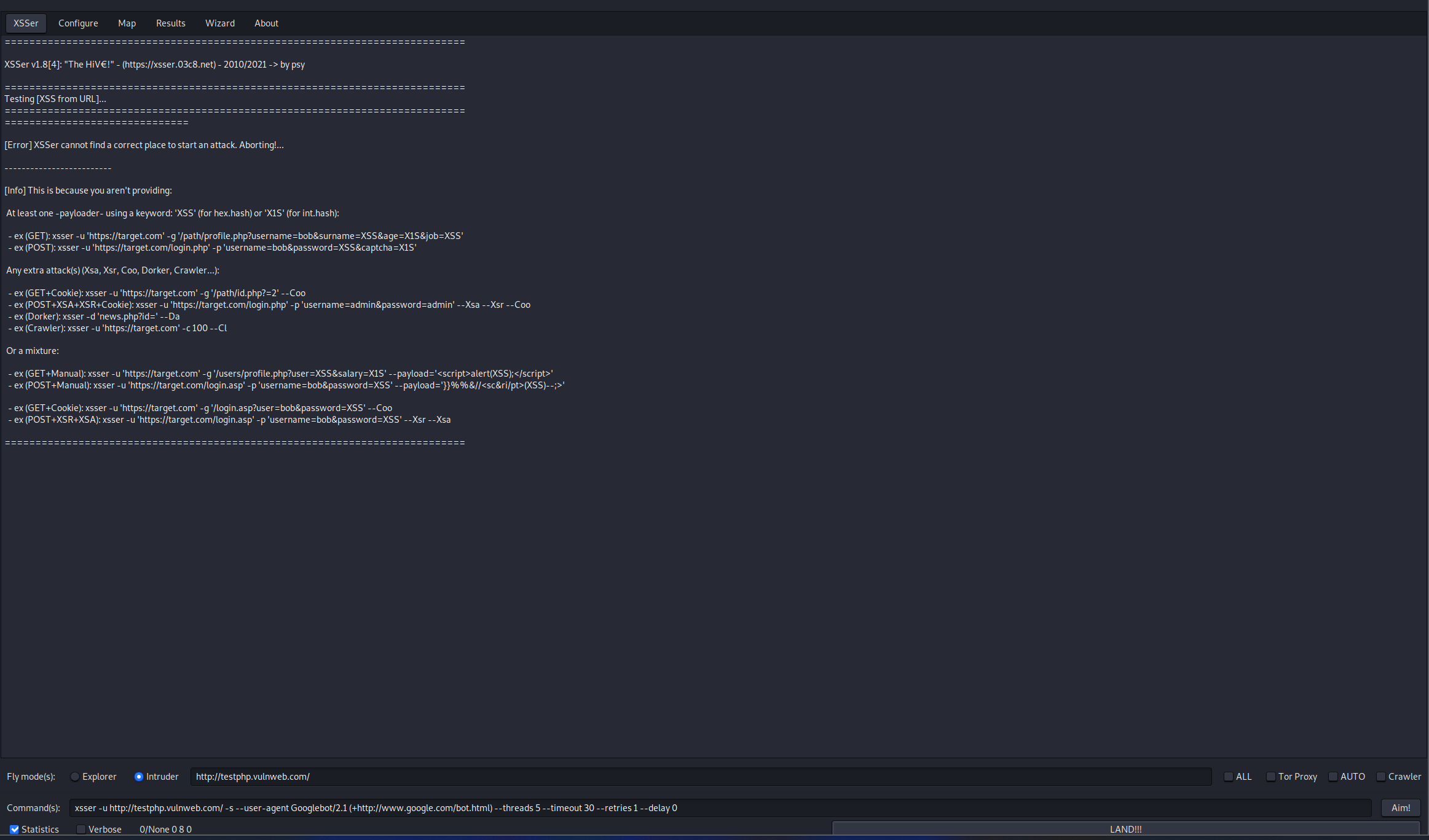


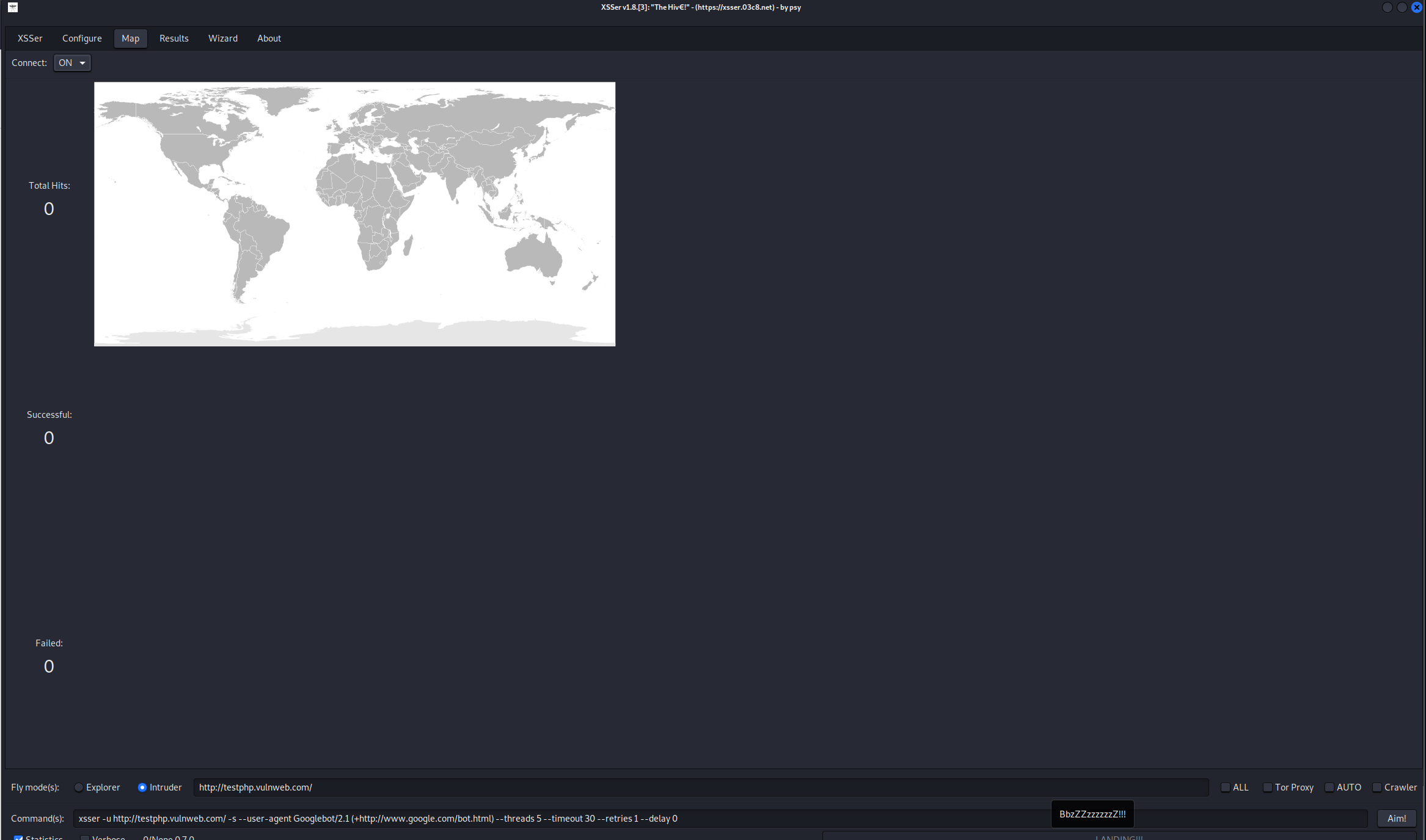
* Now we would be able to see that the request has been forwarded and can also alter the database info.



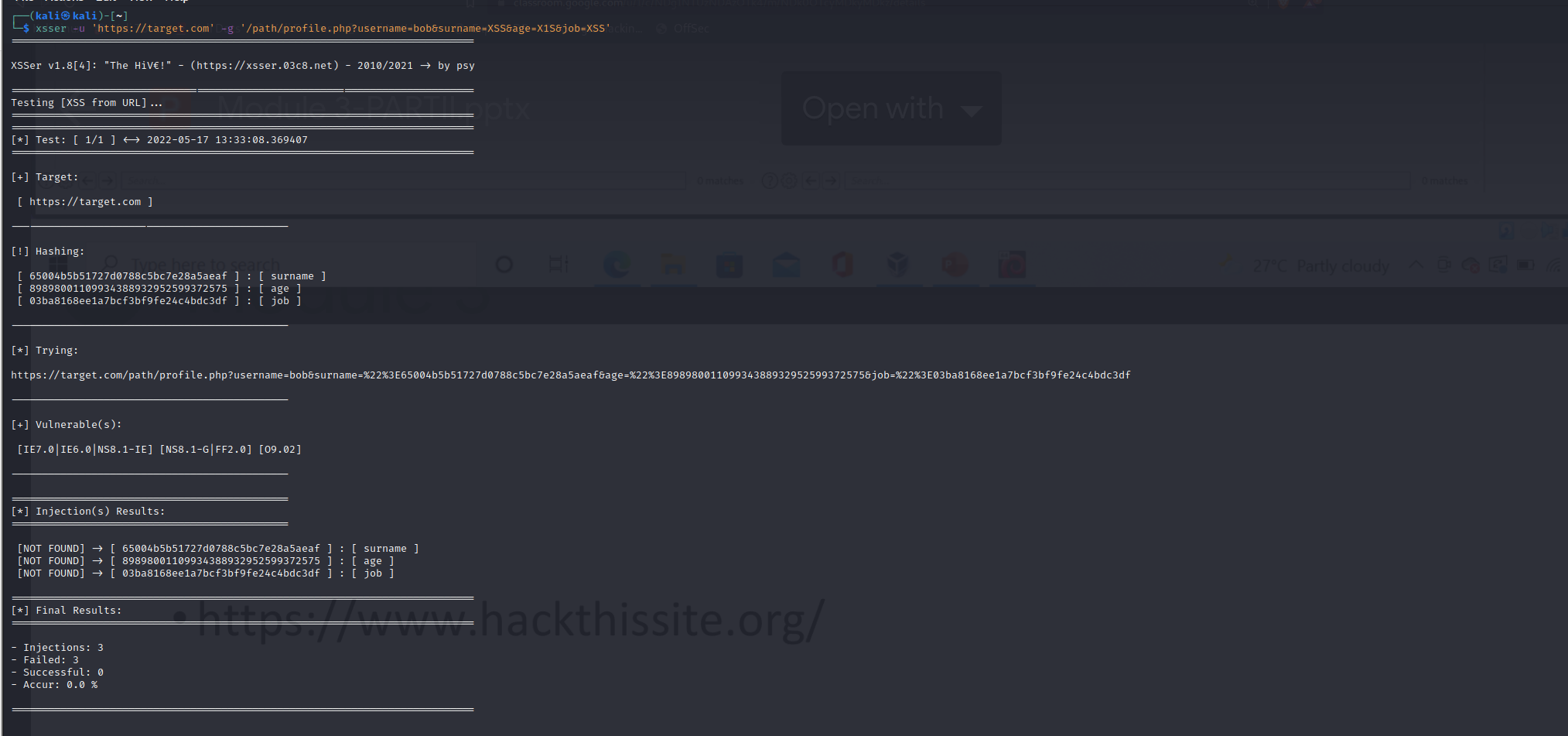
**Perform XSS attack with XSSer.**



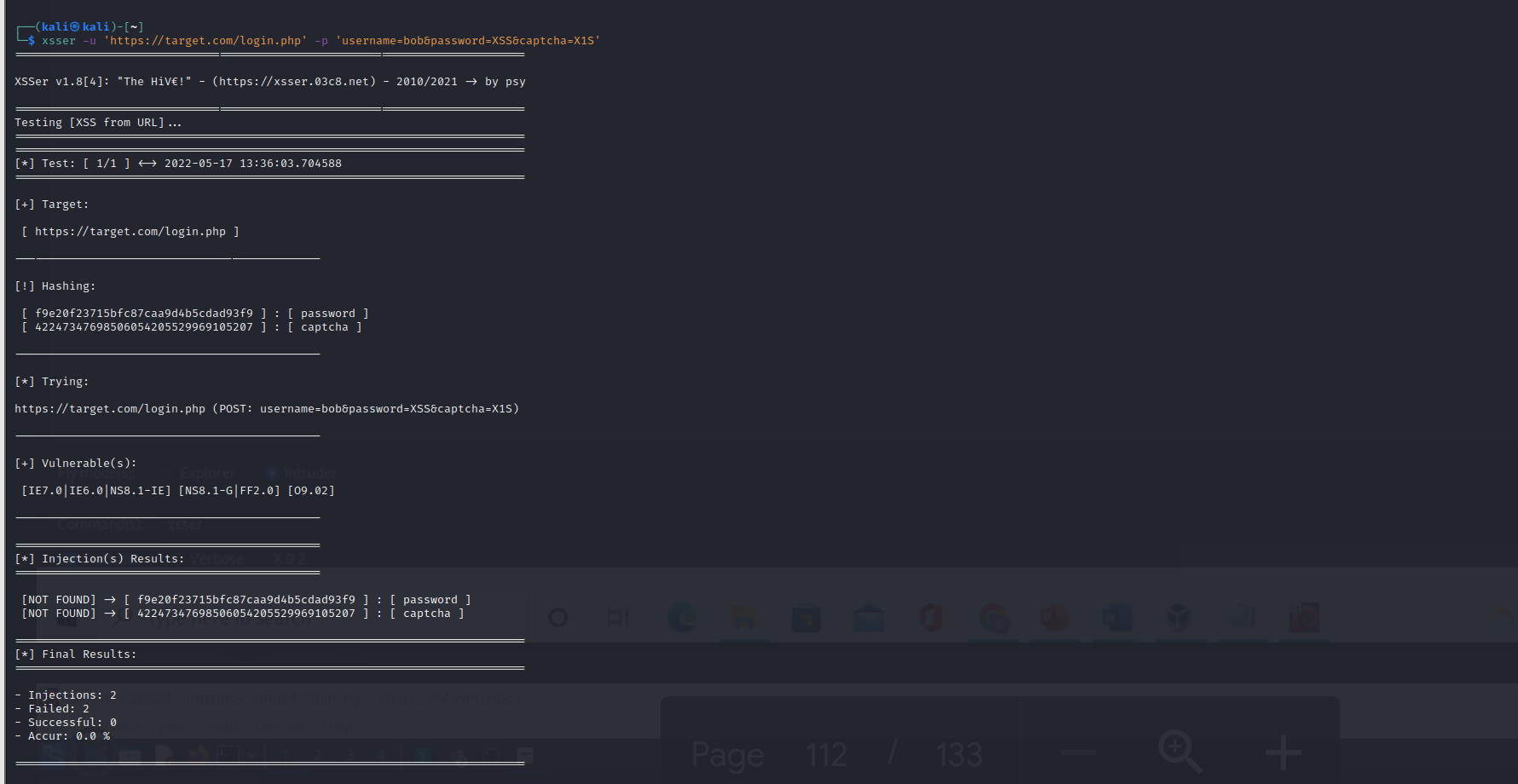




At least one -payloader- using a keyword: 'XSS' (for hex.hash) or 'X1S' (for int.hash):

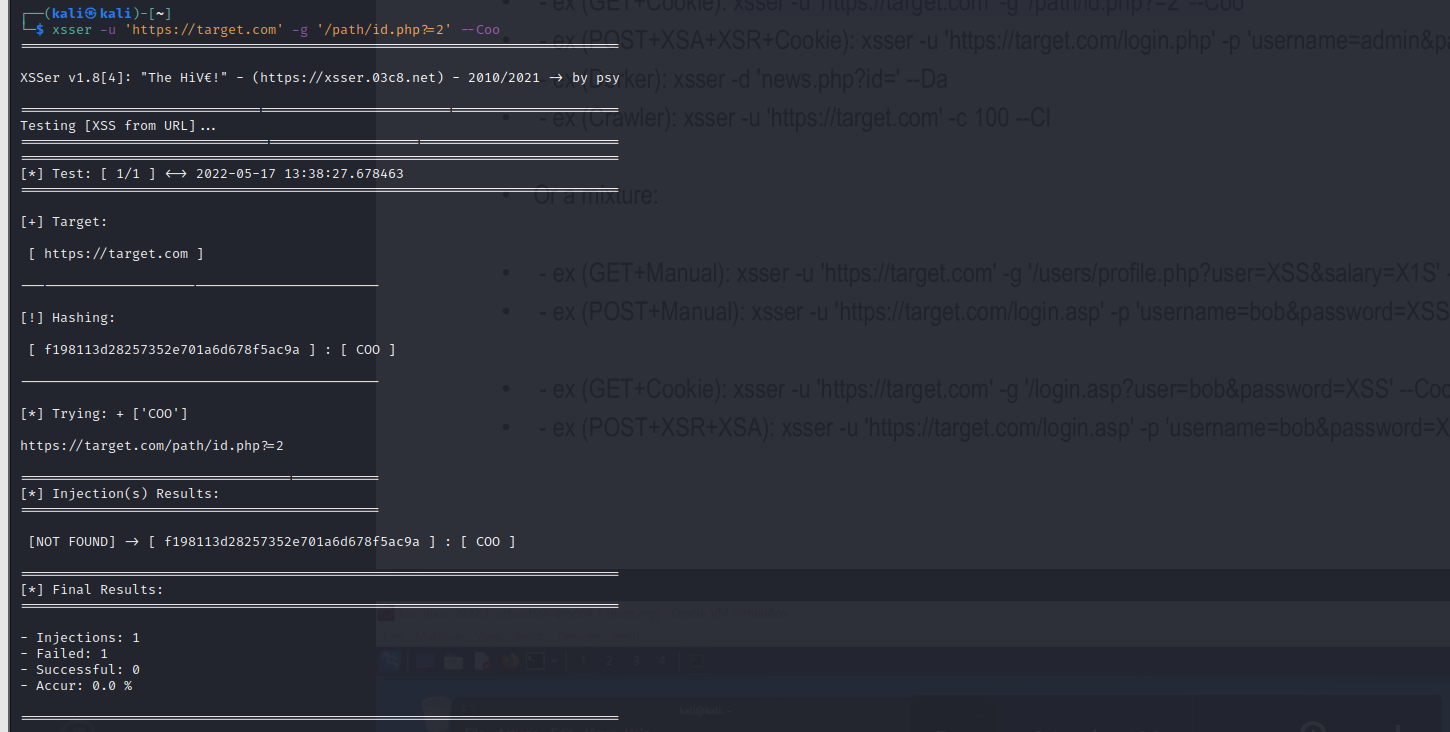
Get method:

Post method:



Any extra attack(s) (Xsa, Xsr, Coo, Dorker, Crawler...):

ex (GET+Cookie):



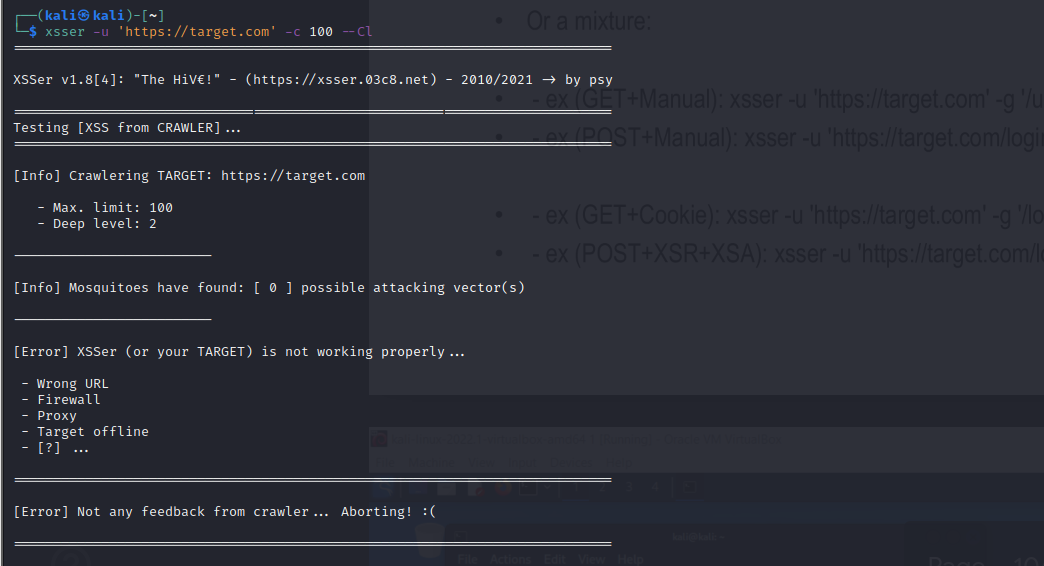
ex (POST+XSA+XSR+Cookie):



ex(Dorker):

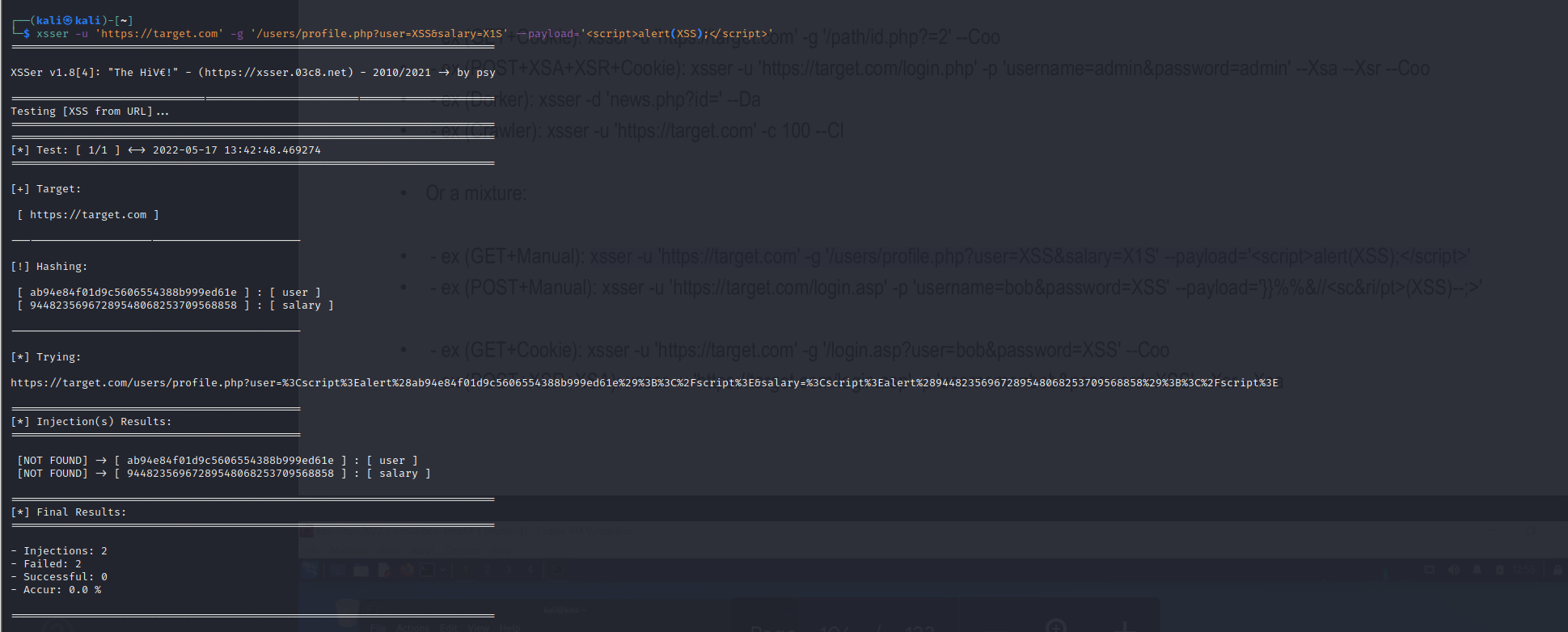


ex (Crawler):

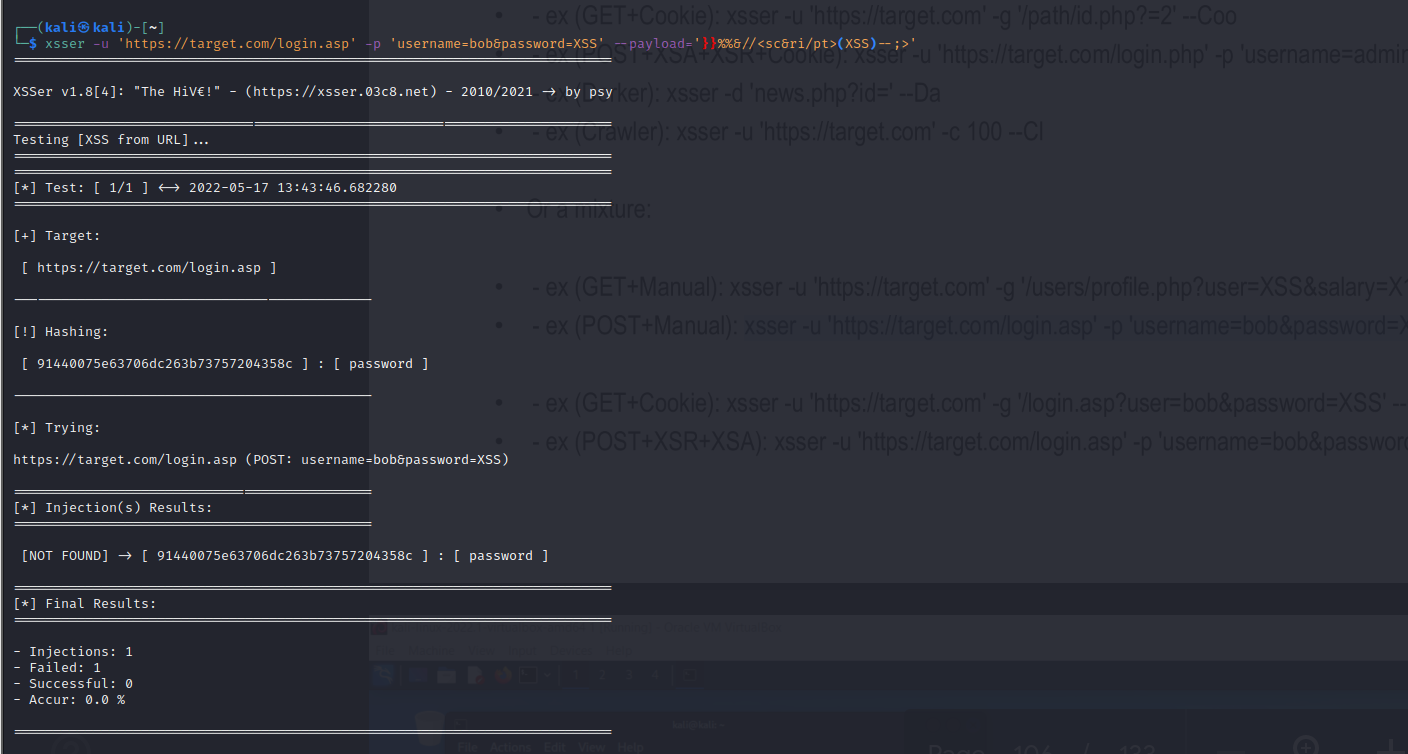


Mixture:

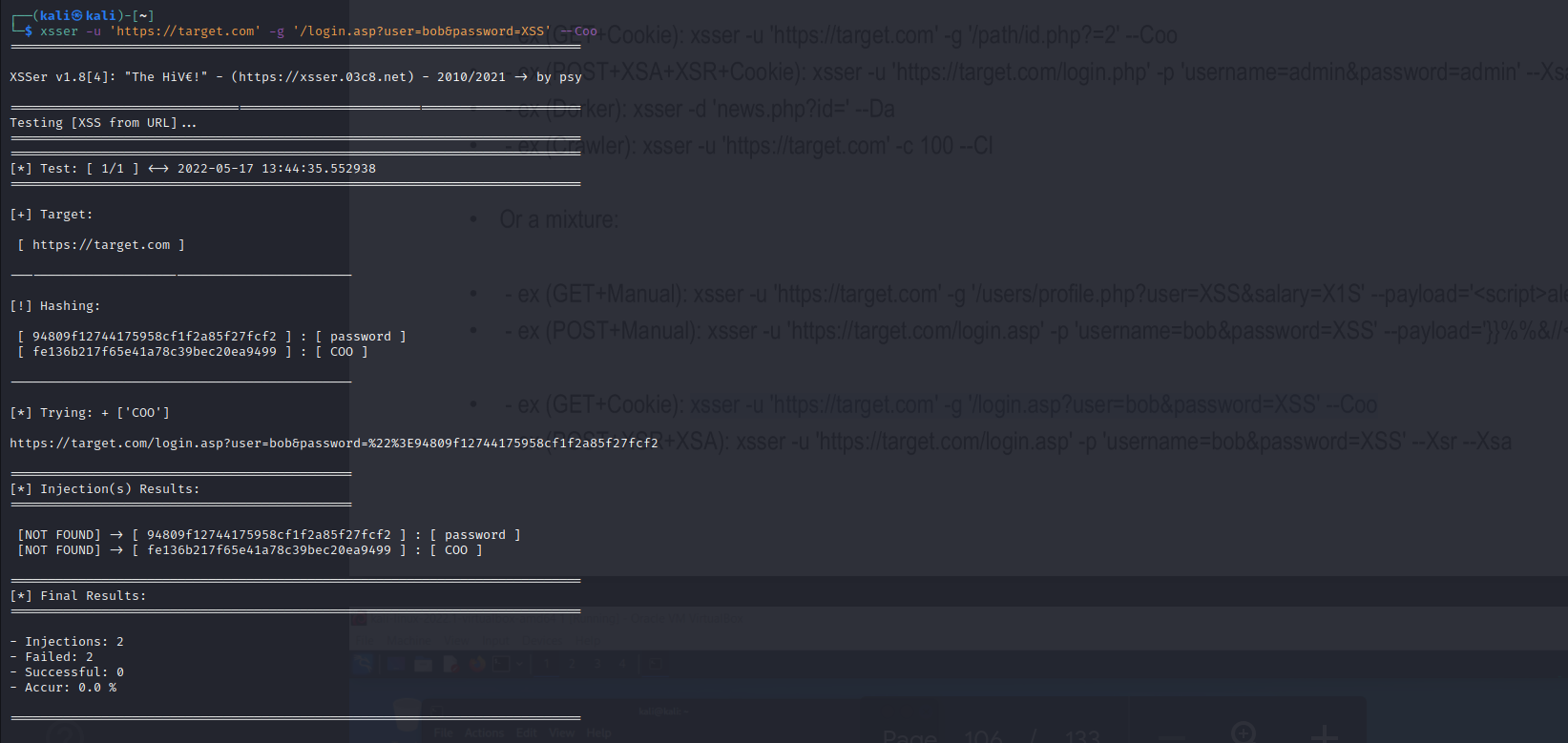
ex (GET+Manual):



ex (POST+Manual):



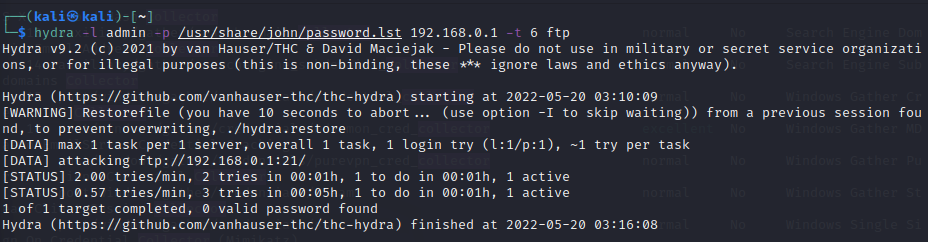
ex (GET+Cookie):



ex (POST+XSR+XSA):



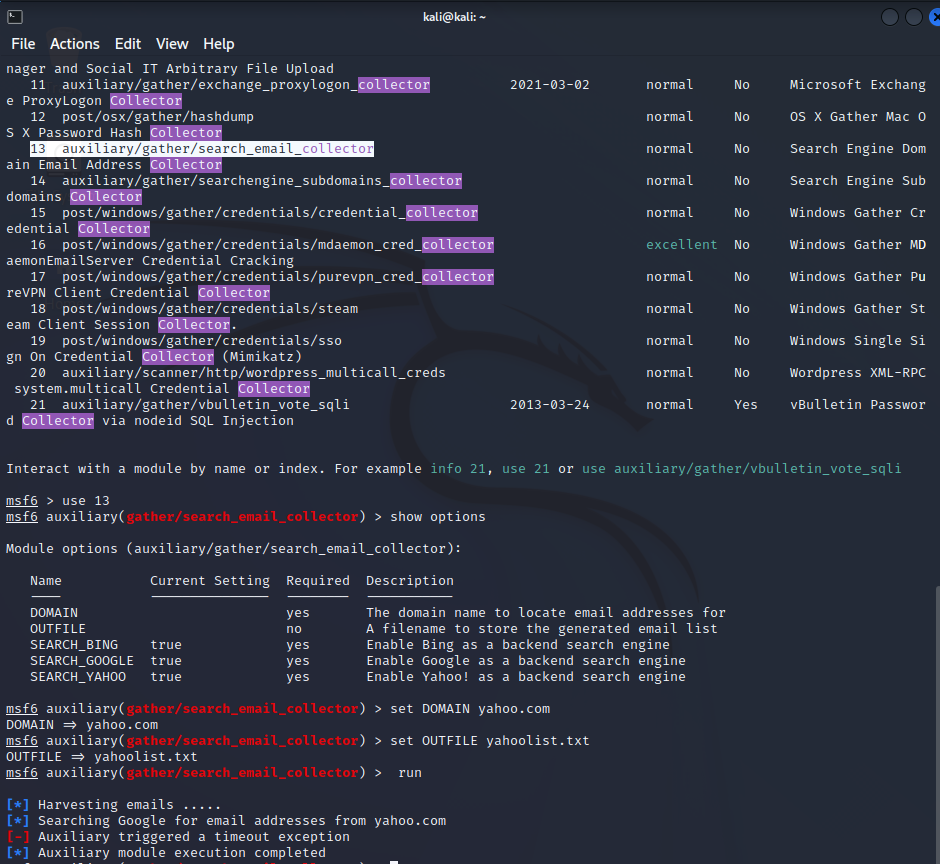
**Perform Brute force attack using Hydra on** [**ftp://192.168.0.1**](ftp://192.168.0.1)

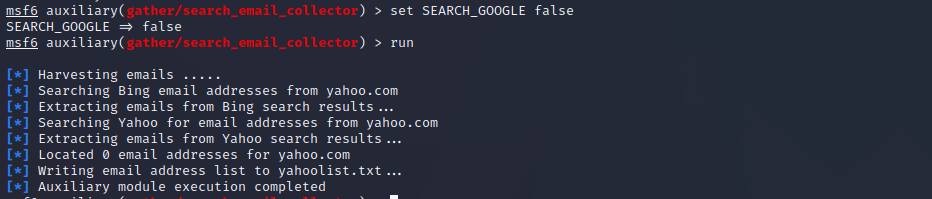
****

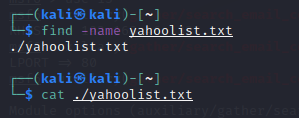
**4. Perform tracking of email locations and harvest emails of yahoo and facebook.**



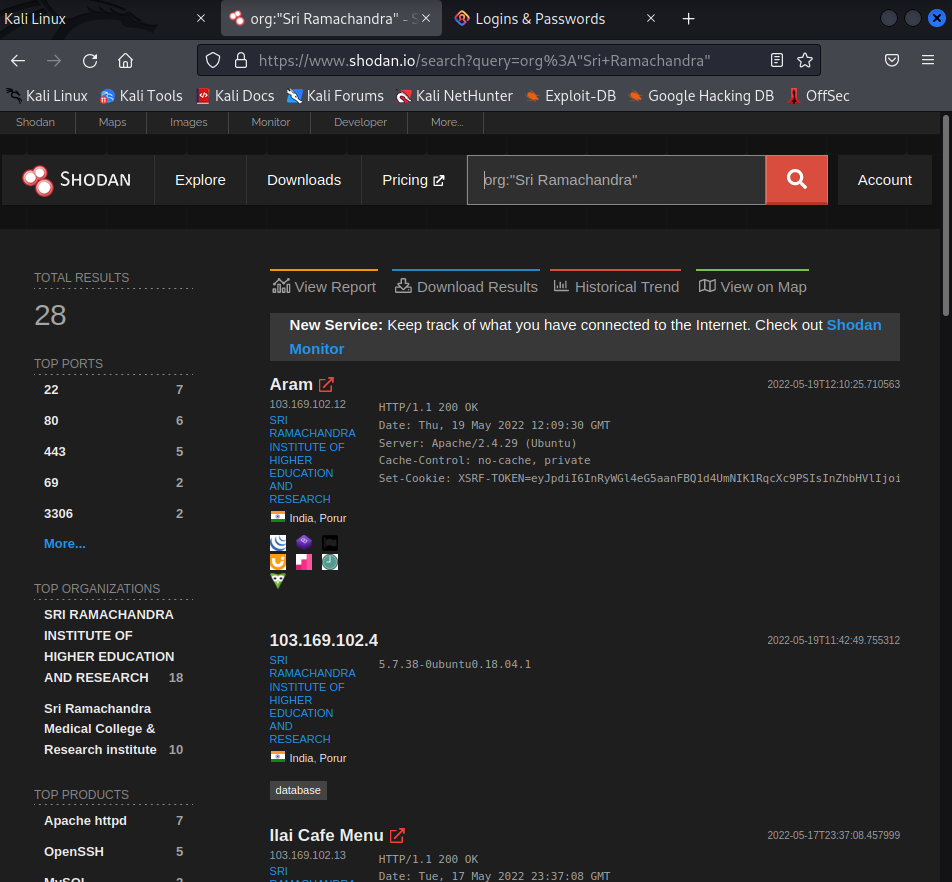


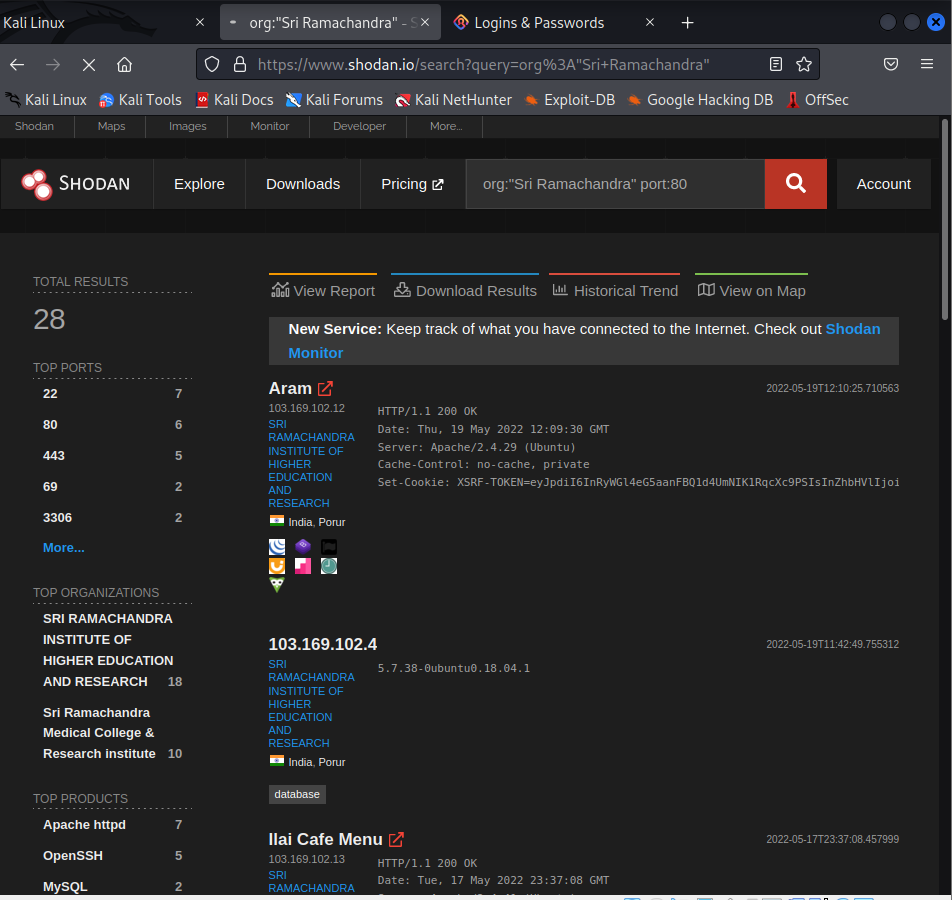






**Using shadon perform the IP address and port search for our SRET.**

****

****